

Amendments to the Claims

1 Claim 1 (currently amended): In a computing environment having a plurality of secure network
2 connections ~~connection to a network~~, a computer program product for securely propagating
3 security credentials using a trusted master registry, the computer program product embodied on
4 one or more computer-readable media and comprising:

5 ~~computer-readable program code means for establishing a secure connection between a~~
6 ~~client and a password synchronization agent (PSA);~~

7 computer-readable program code means for receiving, ~~at the PSA~~ by a password
8 synchronization agent ("PSA") from a user at a [[the]] client device over [[the]] a first secure
9 connection between the client device and the PSA on which the PSA has authenticated itself to
10 the client device, a password propagation request providing an identifier of [[a]] the user and an
11 identifying secret of the user during propagation request processing;

12 computer-readable program code means for ~~validating the user with the~~ forwarding, by
13 the PSA to a trusted master registry over a second secure connection therebetween on which the
14 trusted master registry has authenticated itself to the PSA, [[using]] the received user identifier
15 and identifying secret, on request of the PSA wherein the trusted master registry stores
16 identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

17 computer-readable program code means for receiving, by the PSA from the trusted master
18 registry over the second connection, a validation result created by the trusted master registry
19 responsive to the forwarding, the validation result being a successful result if it indicates that the
20 trusted master registry had previously stored, for the user identifier, a secured version of the
21 identifying secret; and

22 computer-readable program code means for propagating, if the validation result is the
23 successful result, the received user identifier and identifying secret of the user directly from the
24 PSA to one or more target registries if the validation succeeds over third mutually-authenticated
25 secure connections, each of the third connections being between the PSA and a distinct one of the
26 target registries, such that each target registry can store, for the user identifier, a secured version
27 of the identifying secret, wherein the secured version stored by the target registries is not required
28 to be identical to the secured version stored at the trusted master registry.

Claims 2 - 3 (canceled)

1 Claim 4 (currently amended): The computer program product according to Claim 1, wherein the
2 trusted master registry stores password synchronization policy information, and wherein the
3 computer-readable program code means for propagating the received identifying secret further
4 comprises computer-readable program code means for identifying the target registries using the
5 stored password synchronization policy information for the user identifier.

1 Claim 5 (currently amended): The computer program product according to Claim 1, wherein the
2 trusted master registry stores password synchronization policy information, and wherein the
3 computer-readable program code means for propagating the received identifying secret further
4 comprises computer-readable program code means for identifying the target registries using the
5 stored password synchronization policy information for a user group of which the user identified
6 by the user identifier is a member.

Serial No. 09/613,983

-4-

Docket RSW9-2000-0044-US1

Claims 6 - 8 (canceled)

1 Claim 9 (currently amended): The computer program product according to Claim 1, wherein the
2 previously-stored secured version of the identifying secret was created, at the trusted master
3 registry, by computer-readable program code means for validating further comprises:

4 ~~computer-readable program code means for performing a security function on a~~
5 previously-received copy of the received identifying secret of the user, wherein the security
6 function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

7 ~~computer-readable program code means for using the received user identifier to locate a~~
8 ~~previously-stored identifying secret of the user which was stored by the master registry; and~~

9 wherein the security function is repeated, at the trusted master registry, on the forwarded
10 identifying secret of the user, after which, if a result thereof is identical to the previously-stored
11 secured version, the trusted master registry then creates the successful result ~~computer-readable~~
12 ~~program code means for concluding that the validation succeeds if the located identifying secret~~
13 ~~is identical to a result of performing the security function.~~

1 Claim 10 (currently amended): The computer program product according to Claim 1, wherein
2 the validation result is created, at the trusted master registry, by computer-readable program code
3 ~~means for validating further comprises computer-readable program code means for invoking an~~
4 ~~authenticated LDAP bind or other native authentication mechanism of the trusted master registry,~~
5 using wherein the received forwarded user identifier of the user and the received identifying

Serial No. 09/613,983

-5-

Docket RSW9-2000-0044-US1

6 secret of the user, and wherein the validation result is created using a result of the LDAP bind or
7 other native authentication mechanism ~~are passed to the master registry, thereby causing the~~
8 ~~master registry to validate the passed identifier and identifying secret and return a result which~~
9 ~~reports a success or failure of the validation.~~

1 Claim 11 (original): The computer program product according to Claim 1, wherein the PSA has
2 administrative authority for performing operations at the one or more target registries.

1 Claim 12 (currently amended): The computer program product according to Claim 1, further
2 comprising:

3 computer-readable program code means for obtaining a new value from the user to be
4 used as the propagated identifying secret if the validation ~~succeeds~~ result is the successful result;
5 and

6 computer-readable program code means for substituting this new value for the received
7 identifying secret prior to operation of the computer-readable program code means for
8 propagating.

1 Claim 13 (currently amended): A system for securely synchronizing security credentials using a
2 trusted master registry, comprising:

3 ~~means for establishing a secure connection between a client and a password~~
4 ~~synchronization agent (PSA);~~

5 means for receiving, at the PSA by a password synchronization agent ("PSA") from a

6 user at a [[the]] client device over [[the]] a first secure connection between the client device and
7 the PSA on which the PSA has authenticated itself to the client device, a password propagation
8 request providing an identifier of [[a]] the user and an identifying secret of the user during
9 propagation request processing;

10 means for validating the user with the forwarding, by the PSA to a trusted master registry
11 over a second secure connection therebetween on which the trusted master registry has
12 authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, on
13 request of the PSA wherein the trusted master registry stores identifying secrets for user
14 identifiers only as secured, non-recoverable versions thereof;

15 means for receiving, by the PSA from the trusted master registry over the second
16 connection, a validation result created by the trusted master registry responsive to the forwarding,
17 the validation result being a successful result if it indicates that the trusted master registry had
18 previously stored, for the user identifier, a secured version of the identifying secret; and

19 means for propagating, if the validation result is the successful result, the received user
20 identifier and identifying secret of the user directly from the PSA to one or more target registries
21 if the validation succeeds over third mutually-authenticated secure connections, each of the third
22 connections being between the PSA and a distinct one of the target registries, such that each
23 target registry can store, for the user identifier, a secured version of the identifying secret,
24 wherein the secured version stored by the target registries is not required to be identical to the
25 secured version stored at the trusted master registry.

Claims 14 - 15 (canceled)

Serial No. 09/613,983

-7-

Docket RSW9-2000-0044-US1

1 Claim 16 (currently amended): The system according to Claim 13, wherein the trusted master
2 registry stores password synchronization policy information, and wherein the means for
3 propagating ~~the received identifying secret~~ further comprises means for identifying the target
4 registries using the stored password synchronization policy information for the user identifier.

1 Claim 17 (currently amended): The system according to Claim 13, wherein the trusted master
2 registry stores password synchronization policy information, and wherein the means for
3 propagating ~~the received identifying secret~~ further comprises means for identifying the target
4 registries using the stored password synchronization policy information for a user group of which
5 the user identified by the user identifier is a member.

Claims 18 - 20 (canceled)

1 Claim 21 (currently amended): The system according to Claim 13, wherein the previously-stored
2 secured version of the identifying secret was created, at the trusted master registry, by means for
3 validating further comprises:
4 ~~_____~~ means for performing a security function on a previously-received copy of the received
5 identifying secret of the user, wherein the security function comprises one of (i) a one-way
6 hashing algorithm or (ii) an encryption algorithm;
7 ~~means for using the received user identifier to locate a previously-stored identifying~~
8 ~~secret of the user which was stored by the master registry, and~~

Serial No. 09/613,983

-8-

Docket RSW9-2000-0044-US1

9 wherein the security function is repeated, at the trusted master registry, on the forwarded
10 identifying secret of the user, after which, if a result thereof is identical to the previously-stored
11 secured version, the trusted master registry then creates the successful result means for
12 concluding that the validation succeeds if the located identifying secret is identical to a result of
13 performing the security function.

1 Claim 22 (currently amended): The system according to Claim 13, wherein the validation result
2 is created, at the trusted master registry, by means for validating further comprises means for
3 invoking an authenticated LDAP bind or other native authentication mechanism of the trusted
4 master registry, using the forwarded user wherein the received identifier of the user and the
5 received identifying secret of the user, and wherein the validation result is created using a result
6 of the LDAP bind or other native authentication mechanism are passed to the master registry,
7 thereby causing the master registry to validate the passed identifier and identifying secret and
8 return a result which reports a success or failure of the validation.

1 Claim 23 (original): The system according to Claim 13, wherein the PSA has administrative
2 authority for performing operations at the one or more target registries.

1 Claim 24 (currently amended): The system according to Claim 13, further comprising:
2 means for obtaining a new value from the user to be used as the propagated identifying
3 secret if the validation succeeds result is the successful result; and
4 means for substituting this new value for the received identifying secret prior to operation

5 of the means for propagating.

1 Claim 25 (currently amended): A computer-implemented method for securely propagating
2 security credentials using a trusted master registry, comprising steps of:

3 establishing a secure connection between a client and a password synchronization agent
4 (PSA);

5 receiving, by a password synchronization agent ("PSA") at the PSA from a user at a
6 [[the]] client device over [[the]] a first secure connection between the client device and the PSA
7 on which the PSA has authenticated itself to the client device, a password propagation request
8 providing an identifier of [[a]] the user and an identifying secret of the user during propagation
9 request processing;

10 forwarding, by the PSA to a validating the user with the trusted master registry over a
11 second secure connection therebetween on which the trusted master registry has authenticated
12 itself to the PSA, [[using]] the received user identifier and identifying secret, on request of the
13 PSA wherein the trusted master registry stores identifying secrets for user identifiers only as
14 secure, non-recoverable versions thereof;

15 receiving, by the PSA from the trusted master registry over the second connection, a
16 validation result created by the trusted master registry responsive to the forwarding, the
17 validation result being a successful result if it indicates that the trusted master registry had
18 previously stored, for the user identifier, a secured version of the identifying secret; and

19 propagating, if the validation result is the successful result, the received user identifier
20 and identifying secret of the user directly from the PSA to one or more target registries if the

21 ~~validation succeeds over third mutually-authenticated secure connections, each of the third~~
22 ~~connections being between the PSA and a distinct one of the target registries, such that each~~
23 ~~target registry can store, for the user identifier, a secured version of the identifying secret.~~

Claims 26 - 27 (canceled)

1 Claim 28 (currently amended): The method according to Claim 25, wherein the trusted master
2 registry stores password synchronization policy information, and wherein the ~~step of propagating~~
3 ~~step the received identifying secret~~ further comprises the step of identifying the target registries
4 using the stored password synchronization policy information for the user identifier.

1 Claim 29 (currently amended): The method according to Claim 25, wherein the trusted master
2 registry stores password synchronization policy information, and wherein the ~~step of propagating~~
3 ~~step the received identifying secret~~ further comprises the step of identifying the target registries
4 using the stored password synchronization policy information for a user group of which the user
5 identified by the user identifier is a member.

Claims 30 - 32 (canceled)

1 Claim 33 (currently amended): The method according to Claim 25, wherein the previously-
2 stored secured version of the identifying secret was created, at the trusted master registry, by step
3 of validating further comprises:

Serial No. 09/613,983

-11-

Docket RSW9-2000-0044-US1

4 ~~performing a security function on a previously-received copy of the received identifying~~
5 ~~secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm~~
6 ~~or (ii) an encryption algorithm;~~

7 ~~using the received user identifier to locate a previously-stored identifying secret of the~~
8 ~~user which was stored by the master registry; and~~

9 ~~wherein the security function is repeated, at the trusted master registry, on the forwarded~~
10 ~~concluding that the validation succeeds if the located identifying secret of the user, after which, if~~
11 ~~a result thereof is identical to the previously-stored secured version, the trusted master registry~~
12 ~~then creates the successful [[a]] result of performing the security function.~~

1 Claim 34 (currently amended): The method according to Claim 25, wherein the validation result
2 is created, at the trusted master registry, by step of validating further comprises the step of
3 invoking an authenticated LDAP bind or other native authentication mechanism of the trusted
4 master registry, using the forwarded user wherein the received identifier of the user and the
5 received identifying secret of the user, and wherein the validation result is created using a result
6 of the LDAP bind or other native authentication mechanism are passed to the master registry,
7 thereby causing the master registry to validate the passed identifier and identifying secret and
8 return a result which reports a success or failure of the validation.

1 Claim 35 (original): The method according to Claim 25, wherein the PSA has administrative
2 authority for performing operations at the one or more target registries.

1 Claim 36 (currently amended): The method according to Claim 25, further comprising steps of:
2 obtaining a new value from the user to be used as the propagated identifying secret if the
3 validation ~~succeeds~~ result is the successful result; and
4 substituting ~~[[this]]~~ the new value for the received identifying secret prior to operation of
5 the propagating step.

1 Claim 37 (new): The method according to Claim 25, wherein the forwarding and receiving steps
2 use secure interprocess communications between the PSA and the trusted master registry instead
3 of the second connection.

1 Claim 38 (new): The method according to Claim 25, wherein the secured version stored by the
2 target registries is not required to be identical to the secured version stored at the trusted master
3 registry.